

Configure SSH Algorithms

OPERATING INSTRUCTIONS

Copyright

© Ericsson AB 2016. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

1	Introduction	1
1.1	Prerequisites	1
2	Procedure	3





1 Introduction

This document describes how to configure a system-wide Secure Shell (SSH) algorithm setting.

1.1 Prerequisites

This section describes the prerequisites, which must be fulfilled before using the procedure.

1.1.1 Conditions

The following conditions must apply:

- The user has the System Security Administrator role.
- The list of wanted set of algorithms is known.
- The user has basic knowledge of cryptography.
- An Ericsson Command-Line Interface (ECLI) session in Exec mode is in progress.





2 Procedure

To configure `selectedCiphers`, `selectedKeyExchanges` or `selectedMacs` for updating a system-wide SSH algorithm setting:

1. Navigate to *Ssh* Managed Object (MO), for example:

```
>dn ManagedElement=NODE06ST,SystemFunctions=1,SecM=1
,Ssh=1
```

2. Enter Config mode:

```
(Ssh=1) >configure
```

3. Is it required to change `selectedCiphers`?

Yes: Continue with next step.

No: Proceed with Step 5.

Note: Strongest SSH ciphers are selected by default.

4. Set attribute `selectedCiphers` to configure ciphers, for example:

```
(config-Ssh=1) >selectedCiphers= [aes256-ctr,aes192-ctr
,aes128-ctr]
```

The string list must follow the constraints stated in datatype `SshAlgorithm` under *Ssh*.

5. Is it required to change `selectedKeyExchanges`?

Yes: Continue with next step.

No: Proceed with Step 7.

Note: Strongest key exchanges are selected by default.

6. Set attributes `selectedKeyExchanges` to configure key exchanges, for example:

```
(config-Ssh=1) >selectedKeyExchanges= [diffie-hellman-gro
up-exchange-sha1,diffie-hellman-group14-sha1]
```

The string list must follow the constraints stated in datatype `SshAlgorithm` under *Ssh*.

7. Is it required to change `selectedMacs`?

Yes: Continue with next step.



No: Proceed with Step 9.

Note: Strongest message authentication codes are selected by default.

8. Set attribute `selectedMacs` to configure message authentication codes, for example:

```
(config-Ssh=1) > selectedMacs= [hmac-ripemd160@openssh.com  
,hmac-ripemd160,hmac-sha1-96]
```

The string list must follow the constraints stated in datatype `SshAlgorithm` under `Ssh`.

9. Commit the settings:

```
(config-Ssh=1) > commit
```

10. Verify the settings:

```
(Ssh=1) > show -v
```

The following is an example output:

```
selectedCiphers  
  "aes256-ctr"  
  "aes192-ctr"  
  "aes128-ctr"  
selectedKeyExchanges  
  "diffie-hellman-group-exchange-sha1"  
  "diffie-hellman-group14-sha1"  
selectedMacs  
  "hmac-ripemd160@openssh.com"  
  "hmac-ripemd160"  
  "hmac-sha1-96"  
[...]
```